Kerberos in Mac OS X

Session 814

Kerberos in Mac OS X

John Hurley, Ph.D.
Manager, Data Security

Introduction

- Overview of the Kerberos authentication system
  - What it is
  - How it works
- Libraries available to developers
- How to add Kerberos to your application

What You Will Learn

- What Kerberos is and where it is used
- How to Kerberize your application

What Is Kerberos?

- A secure network authentication system
  - Authentication vs. Authorization
- Proves who you are
- Uses a trusted third-party model security model

Who Uses Kerberos?

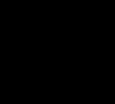
- Government
- Large corporations
- Higher education
- Every Windows 2000 (or later) installation

Why Do They Use It?

- Mutual authentication of client and server
- Single sign on
- Factor security problem (Authentication vs. Authorization)
- Consistent with centralized authentication goals
- Highly extensible/interfaceable
    - RADIUS, PAM, etc.

Why Do They Use It?

- Inherently more secure than any other encrypted password exchange
    - Password never sent over the wire
- Ubiquitous
    - Mac, Win, Solaris, Mac OS X, Linux, HP-UX, AIX . . .
- Time tested
    - Developed in 1980s as part of Project Athena
- Source freely available



Apple and Kerberos

- Important to our markets
- MIT Press Release WWDC 2000
- Kerberos has been available since Mac OS X 10.0
    - Already a large installed base!
    - Mac OS X 10.1 and Kerberos

Kerberos in Jaguar

Components that have been Kerberized

- KfM 4.5 from MIT is the base
- Mac OS X Client
  - AFP
  - Unix utilities: telnet, ftp
  - Mail application
  - Kerberos login authentication

Kerberos in Jaguar Server

Components that have been Kerberized

- Mac OS X Server
  - AFP server
  - Mail server
  - FTP server

Demo

Richard Murphy
Manager, Platform Security

Kerberos for Macintosh

Marshall Vale
Project Manager, Macintosh and Kerberos Development
Massachusetts Institute of Technology

Kerberos Protocols

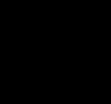
- Kerberos v4
  - Original version, no longer developed
  - Still in use at many long-standing Kerberos sites
- Kerberos v5
  - Current version of the protocol
  - Designed to solve many deficiencies and security problems in v4

Kerberos Terms

- Realm
  - The administrative unit protected by a Key Distribution Center (KDC)
- Ticket
  - An authentication token
- Ticket-granting ticket (TGT)
  - An initial ticket that grants permission to get service tickets
- Service ticket
  - A ticket that authenticates the user to a particular service (e.g., ftp, mail, telnet)

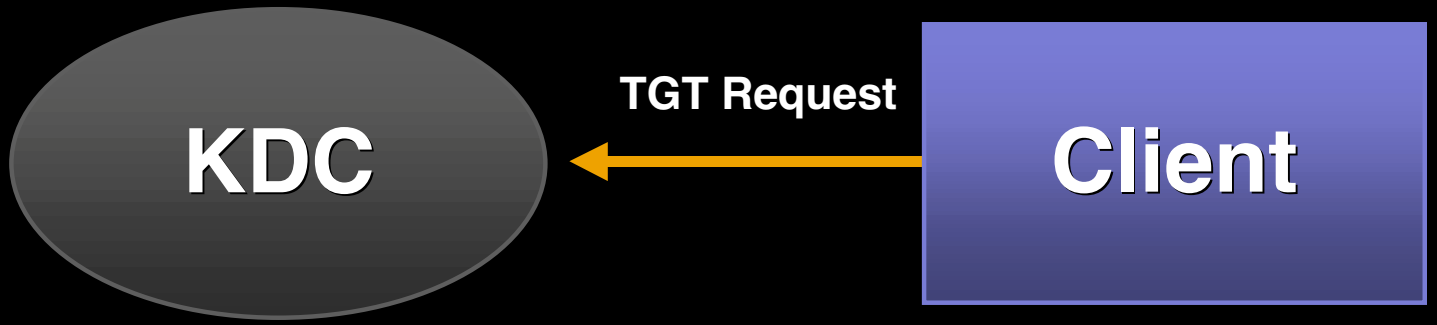
Ticket-Granting Ticket (TGT)

- Also called “initial ticket” because it is the first ticket a client gets
- Proves that the client is allowed to get tickets for other services
- Acts as a substitute for password
- Mechanism by which single sign on is achieved
- Only valid for a limited period of time (expires)



Getting a TGT

- Client asks KDC for TGT

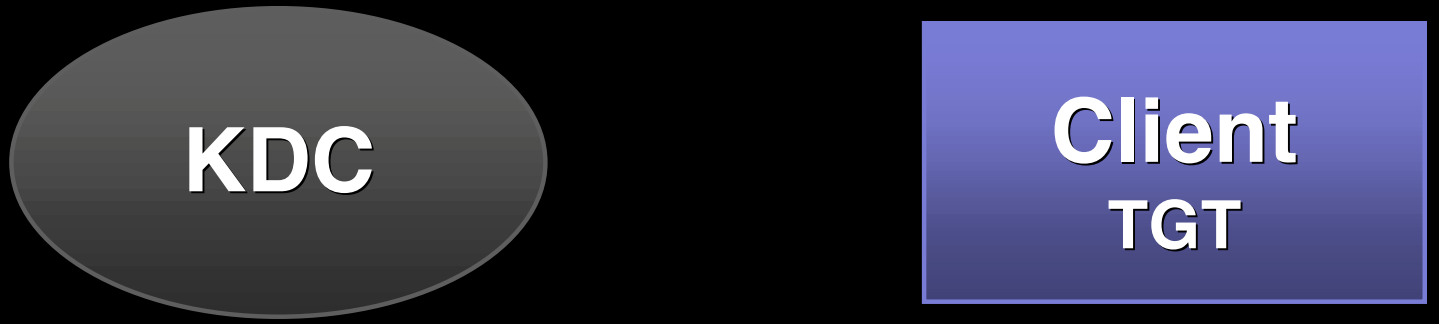


Getting a TGT

- KDC returns a TGT and session key to a client encrypted with client's key

Getting a TGT

- Client uses client's key (one-way hash of password) to extract TGT

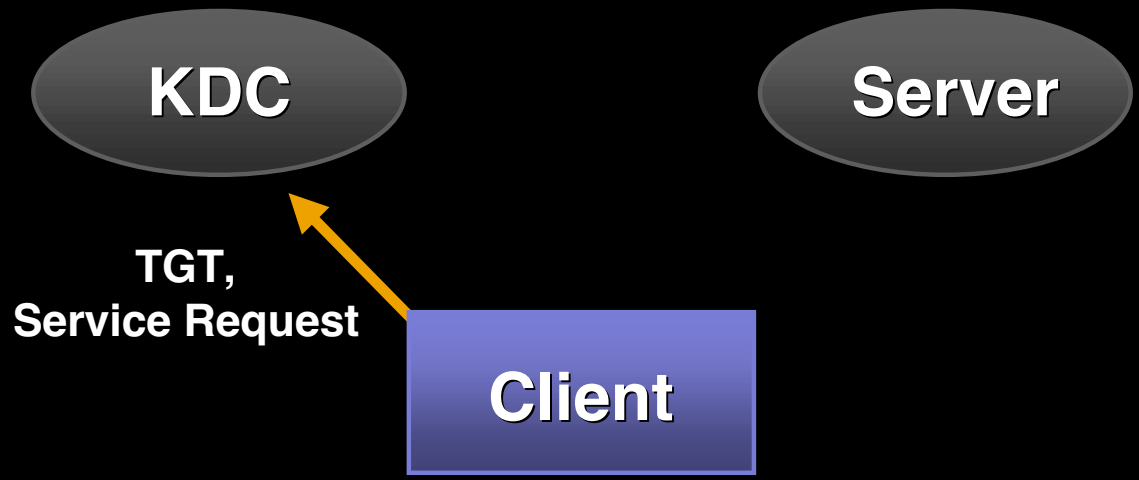


Service Ticket

- Ticket used by client to get access to particular service or server (e.g., ftp, mail, telnet)
- Contains a session key which is shared between the client and server that they can use to encrypt data exchanges
- Also expires

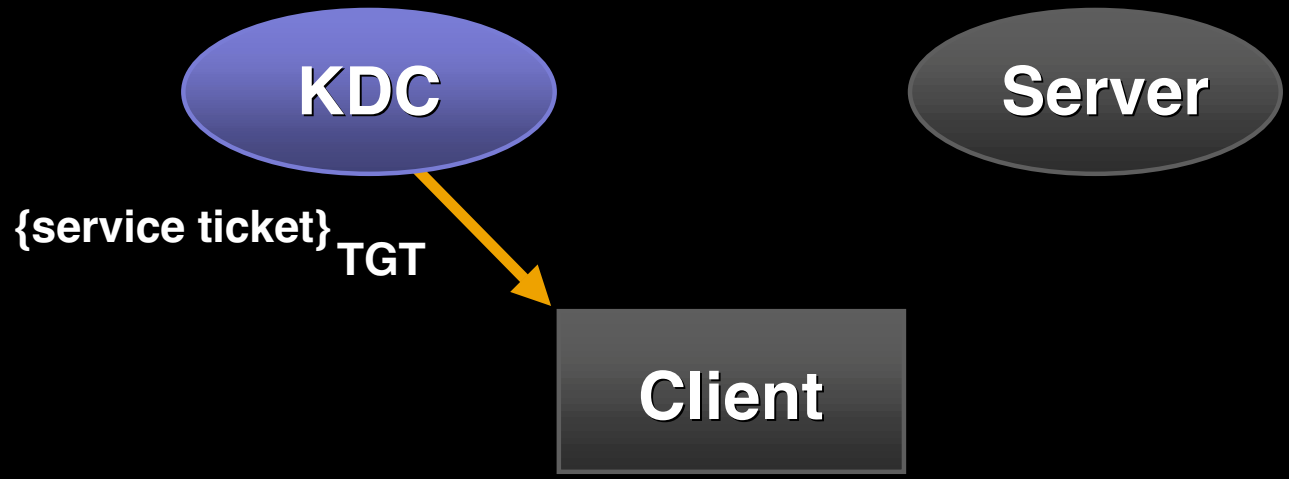
Getting a Service Ticket

- Client presents TGT to KDC with a request for a service ticket



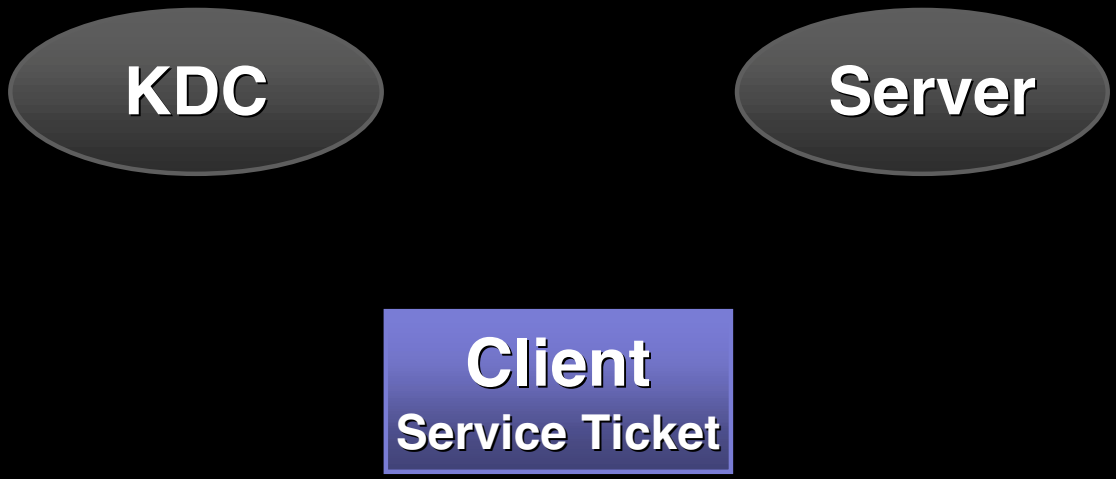
Getting a Service Ticket

- KDC returns encrypted service ticket to client



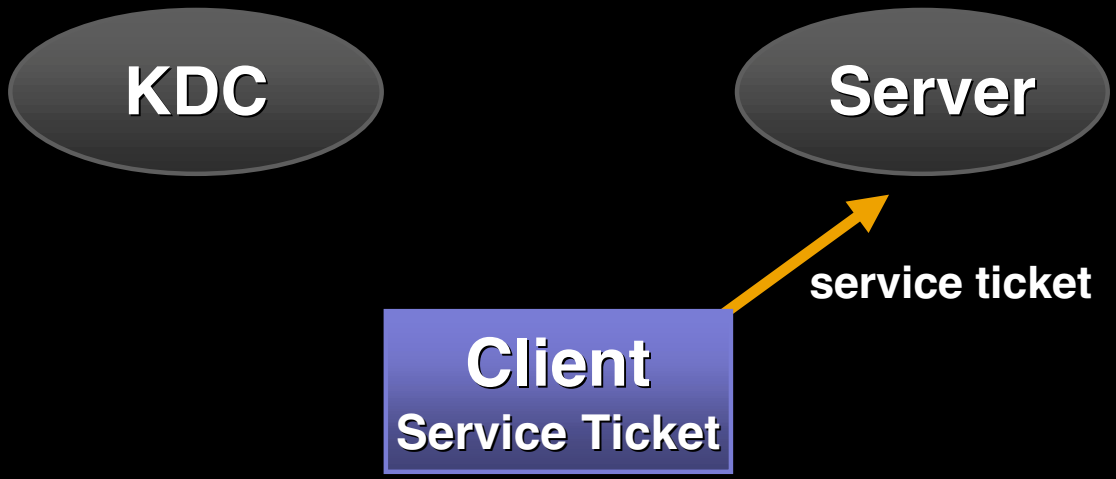
Getting a Service Ticket

- Client uses TGT to extract service ticket



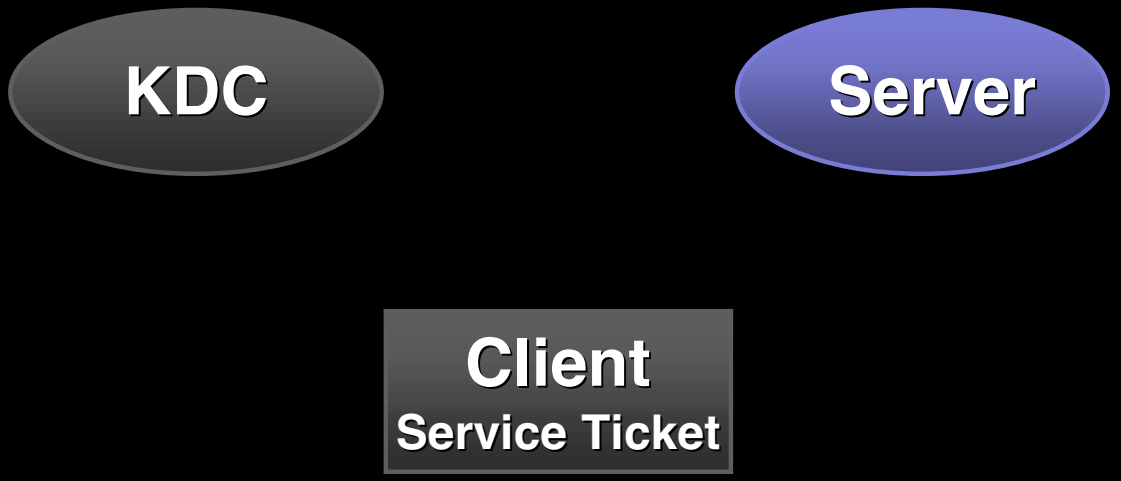
Connecting to a Service: One-way Authentication

- Client presents service ticket to server



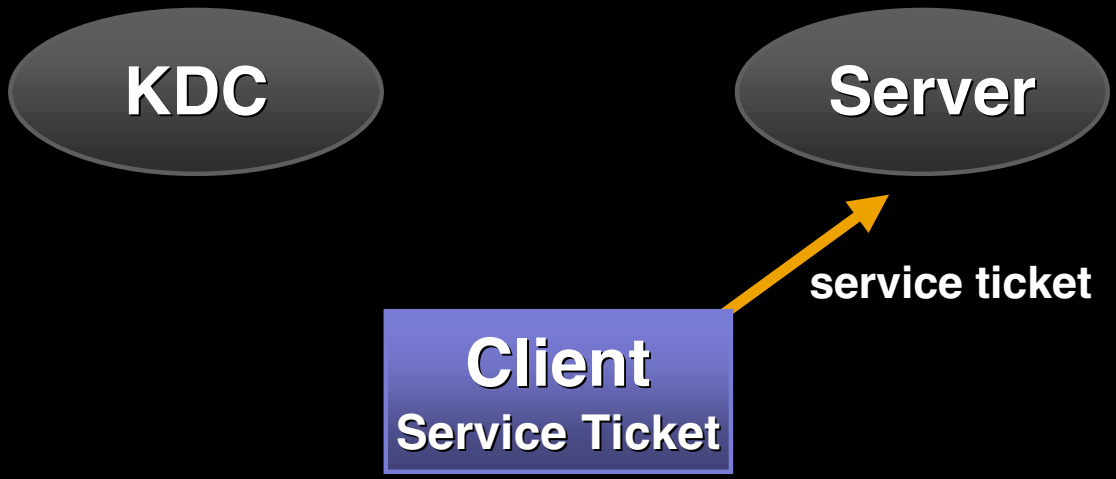
Connecting to a Service: One-way Authentication

- Server receives service ticket and authenticates the client
- Server may use session key from service ticket to encrypt subsequent traffic between client and server



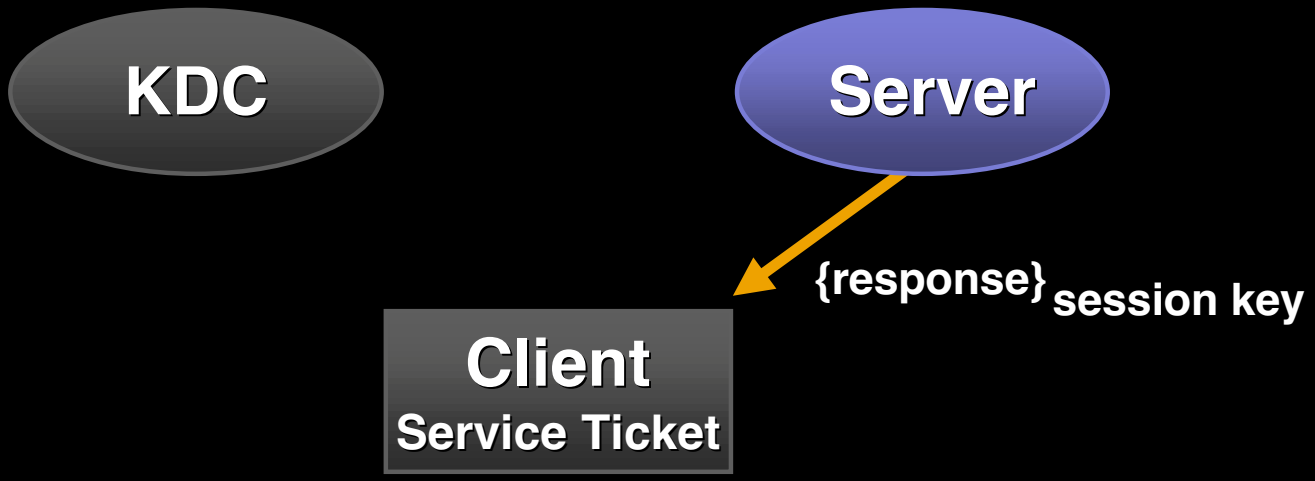
Connecting to a Service: Mutual Authentication

- Client sends service ticket containing session key to server



Connecting to a Service: Mutual Authentication

- Server returns a response encrypted with session key from service ticket, authenticating server to client
- Server may also use session key to encrypt subsequent traffic between client and server



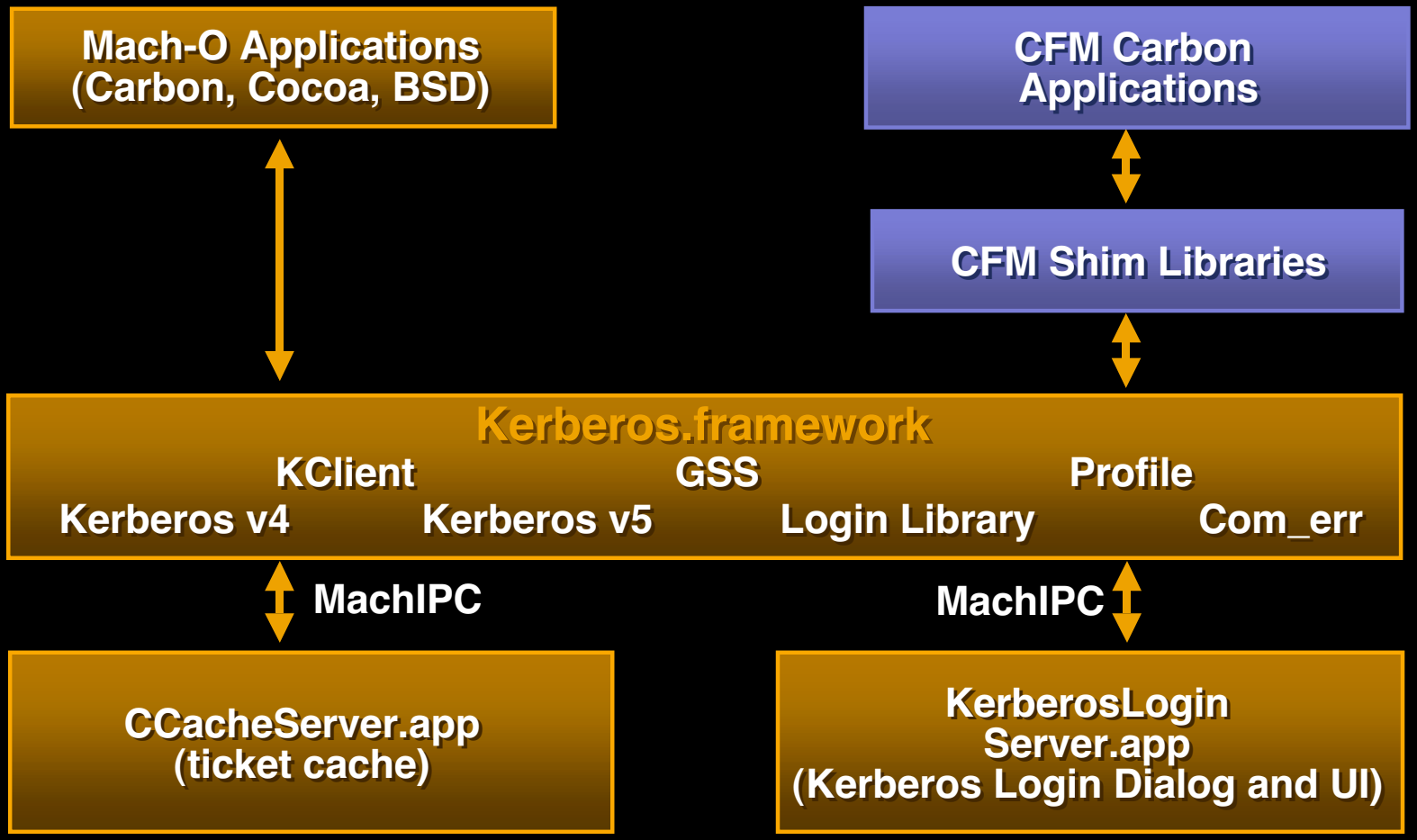
Kerberos for Macintosh 4.0

- Pre-release version included in Mac OS X 10.1
- Supports both Kerberos v4 and v5
- Provides Kerberos libraries on Mac OS X
    - Carbon
    - Cocoa
    - Command Line
- Live ticket sharing between Mac OS X and Classic
- Last release for Classic Mac OS

Kerberos for Macintosh 4.5

- Provided only as part of Jaguar
- New features include:
    - Improved loading times
    - Reduced memory usage
    - First version of supportable v5 API
    - 524 support
    - kswitch
- No release for Mac OS 9

KfM 4.5 Architecture



Kerberos v4

- KClient 3.1
  - Compatibility libraries
  - New version 3 APIs
- Cygnus Kerberos v4 implementation
  - The final Cygnus release (version 96q4)
  - Modifications to support KerberosLoginLibrary
- Applications can use either API for v4 calls
  - KClient 3 APIs recommended
  - Historic v4 API only for porting existing Kerberos code

Kerberos v5

- MIT Kerberos v5 1.2.5
  - New cross-platform API suite
- GSSAPI
  - Supports RFC #1509—"Generic Security Service API : C-bindings" and RFC #1964—"The Kerberos Version 5 GSS-API Mechanism"

Microsoft Interoperability

- Active Directory can be used as a Kerberos v5 KDC to Mac OS X Kerberos clients
- Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) currently has no counterpart on Mac OS X
- Security Support Provider Interface (SSPI) is very similar to GSSAPI

Credentials Cache

- Bottom layer—where the tickets/credentials are stored
- Stored in memory as opposed to on disk
    - More efficient flexibility in handling multiple credentials
- Provides API for accessing the credentials used by KClient, v4, v5 libraries

Kerberos Login Library

- Simplifies the process of getting Kerberos TGTs
  - Allows you to get or destroy tickets with a single call
  - Transparently handles v4 and v5 initial tickets
- Also provides API for adjusting Kerberos Login Dialog options
- Used by programs that need to perform actions on TGTs, such as administrative applications

Other Libraries

- Com_err
  - Access error codes returned by Kerberos
- Profile
  - Read information stored in the Kerberos configuration file (e.g., library defaults, realms, etc.)

Kerberos Application

- Provides a UI for obtaining, destroying, listing, and displaying information about tickets and currently authenticated users
- Also provides UI for setting
  - Kerberos Login dialog options
  - Favorite realm
- Dock icon presents ticket status and menu

How to Kerberize an Application

- Find the protocol specification (RFCs, etc.)
- Determine which API to use (KClient, Kerberos v5, GSSAPI, etc.)
- Figure out how to connect the API to the protocol
    - The data returned by the API usually needs to be massaged into a form required by the protocol

Kerberizing FTP

- Protocol: RFC 2228, RFC 959
- Supports Kerberos v4 and GSS
    - Use KClient for Kerberos v4 (better support for multiple sessions)
    - Use GSSAPI for Kerberos v5

Kerberizing FTP: Kerberos v4

- Session management
  - **KClientNewClientSession**
- Authentication
  - **KClientGetAuthenticatorForService**
  - **KClientVerifyProtectedServiceReply**
- Encryption and decryption
  - **KClientEncrypt**
  - **KClientDecrypt**
- Connecting the API to the protocol
  - Base 64 encoding

Kerberizing FTP: GSSAPI

- Session management and authentication
  - **gss_init_sec_context**
- Encryption and decryption
  - **gss_wrap**
  - **gss_unwrap**
- Connecting the API to the protocol
  - Base 64 encoding

How Do I Get Started?

- Use Kerberos for Macintosh 4.5 provided in Jaguar
- Development version included in the Jaguar CDs
- Use online resources—web documentation, mailing lists and newsgroups for assistance

Reporting Bugs

- Send bugs in KfM 4.0 to MIT
  krb5-bugs@mit.edu
- File bugs about Kerberos in Jaguar with Apple

For More Information

- MIT Kerberos for Macintosh
  http://web.mit.edu/macdev/www/kerberos.html
- Kerberos Papers and Documentation
  http://web.mit.edu/kerberos/www/papers.html
- Kerberos for Macintosh Development Team
  macdev@mit.edu
- Kerberos Development List
  krbdev-request@mit.edu

For More Information

- Internet RFCs
  http://www.ietf.org/rfc.html
- Describing GSSAPI in terms of SSPI
  http://msdn.microsoft.com/library/techart/sspikerberos.htm
- Usenet
  comp.protocols.kerberos

Who to Contact

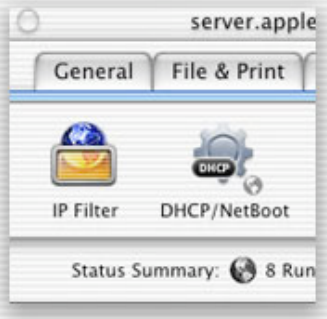
Tom Weyer
Network and Communications Technology Manager
weyer@apple.com

Marshall Vale
Project Manager: Macintosh and Kerberos Development
Massachusetts Institute of Technology
mjv@mit.edu

Craig Keithley
Security and Cryptography Technology Manager
keithley@apple.com

http://developer.apple.com/wwdc2002/urls.html

Q&A



Tom Weyer
Network and Communications Evangelist
weyer@apple.com

http://developer.apple.com/wwdc2002/urls.html


WWDC2002


WWDC2002


WWDC2002